IN THE CLAIMS:

Please amend claims as follows:

1. (Currently amended) A method ~~by which~~ for use by a telecommunications terminal (10) in authenticating the telecommunications terminal (10)~~determines whether a candidate RAND included in a RAND challenge is a member of a set of previously used RANDs, characterized by~~ comprising:

~~a step (31) of~~ encoding ~~the~~ random numbers previously used ~~RANDs~~ for authenticating the telecommunications terminal (10), ~~using~~ so as to provide a data structure (21) consisting of an ordered set of components having respective component values derived from the previously used ~~RANDs~~ random numbers, wherein each component has a starting value of zero, but the value ~~of~~ is set to one ~~or zero depending on whether~~ if, based on the order of the component in the ordered set, the component ~~it~~ is pointed to by any of a plurality of ~~one or more pointers each having a value~~ pointer values each based on ~~a digest of~~ all the bits of a respective one of the previously used ~~RAND~~ random numbers~~or having a value otherwise derived from all the components of a respective previously used RAND so that in either case all bits of the RAND contribute in determining the value of the component~~; and

~~a step (32) of~~ checking the data structure (21) to determine whether ~~the data structure indicates whether the~~ a candidate random number ~~RAND~~ is ~~a member of a set of~~ not one of the previously used random numbers ~~RANDs~~;

wherein the data structure (21) is such as to at least provide a true answer as to whether the candidate random number ~~RAND~~ is not ~~an element of the set of~~ one of the previously used random numbers ~~RANDs~~.

2. (Currently amended) A method as in claim 1, wherein in ~~the step (31) of~~ encoding the previously used random numbers ~~RANDs~~, a set of hash functions is used each ~~having~~ providing a value in a range equal to the number of components of the data structure (21), and for each previously used random number ~~RAND~~, each of the hash functions is evaluated and the component in the ordered set of components at the position indicated by the hash function value is set to one.

3. (Currently amended) A method as in claim ~~2~~1, wherein in encoding the previously used random numbers, the previously used random numbers are used as the pointer values~~the previously used RAND values serve as the hash functions based on using the RAND values as pointers to components of the data structure (21)~~.

4. (Currently amended) A method as in claim 1, wherein the data structure (21) is a multi-part data structure (21) with each part having an upper limit on the number of random number ~~RAND~~ values it can indicate as ~~belonging to the set of~~ one of the previously used random number ~~RAND~~ values, wherein each part has values based on only some of the previously used random numbers, and wherein all most recently received random numbers are used in determining component values in only one of the parts, and further wherein when an upper limit is reached for the one of the parts, another of the parts is reset.

5. (Currently amended) A computer program product ~~comprising~~ comprising:

a computer readable storage structure embodying computer program code thereon for execution by a computer processor in a terminal (10),

~~with~~ wherein said computer program code ~~characterized in that it~~ includes instructions for performing the ~~steps of the~~ method of claim 1.

6. (Currently amended) An apparatus ~~included~~ for use by ~~in~~ a telecommunication terminal (10) ~~and by which the telecommunication terminal (10) determines~~ in authenticating the telecommunications terminal (10) to an access network~~whether a candidate RAND included in a RAND challenge is a member of a set of previously used RANDs~~, ~~characterized by~~comprising:

means (11 12 ~~3~~1~~1~~4) for encoding random numbers previously used for authenticating the telecommunications terminal (10), so as to provide a data structure (21) consisting of an ordered set of components having respective component values derived from the previously used random numbers, wherein each component has a starting value of zero, but the value is set to one if, based

on the order of the component in the ordered set, the component is pointed to by any of a plurality of pointer values each based on all the bits of a respective one of the previously used random numbers~~encoding the previously used RANDs using a data structure (21) consisting of an ordered set of components having component values derived from the previously used RANDs wherein each component has a value of one or zero depending on whether it is pointed to by one or more pointers each having a value based on a digest of all the bits of a respective previously used RAND or having a value otherwise derived from all the components of a respective previously used RAND so that in either case all bits of the RAND contribute in determining the value of the component~~; and

means (11 12 ~~32~~14) for checking the data structure (21) to determine whether ~~the data structure indicates whether the~~ a candidate random number~~RAND~~ is ~~a member of a set of~~ not one of the previously used random numbers~~RANDs~~;

wherein the data structure (21) is such as to at least provide a true answer as to whether the candidate random number~~RAND~~ is not ~~an element~~ one of the ~~set of~~ previously used random numbers~~RANDs~~.

7. (Currently amended) A system, comprising:

~~a~~ telecommunication terminal (10), and

a radio access network configured for cellular communication with the telecommunication terminal (10),

wherein ~~characterized in that~~ the telecommunication terminal (10) includes an apparatus as in claim 6.

8. (New) An apparatus for use by a telecommunication terminal (10) in authenticating the telecommunications terminal (10) to an access network, comprising an authenticator module (14) and one or more Bloom filter modules (11 12), configured to:

encode random numbers previously used for authenticating the telecommunications terminal (10), so as to provide a data structure (21) consisting of an ordered set of components having respective component values derived from the previously used random numbers, wherein each component has a starting value of zero, but the value is set to one if, based on the order of the

component in the ordered set, the component is pointed to by any of a plurality of pointer values each based on all the bits of a respective one of the previously used random numbers; and

check the data structure (21) to determine whether a candidate random number is not one of the previously used random numbers;

wherein the data structure (21) is such as to at least provide a true answer as to whether the candidate random number is not one of the previously used random numbers.

9. (New) An apparatus as in claim 8, wherein for encoding the previously used random numbers the authenticator module (14) and one or more Bloom filter modules (11 12) are configured so that a set of hash functions is used each having a range equal to the number of components of the data structure (21), and for each previously used random number, each of the hash functions is evaluated and the component in the ordered set of components at the position indicated by the hash function value is set to one.

10. (New) An apparatus as in claim 8, wherein the previously used random numbers are the pointer values.

11. (New) An apparatus as in claim 8, wherein the data structure (21) is a multi-part data structure (21) with each part having an upper limit on the number of random number values it can indicate as one of the previously used random number values, wherein each part has values based on only some of the previously used random numbers, and wherein all most recently received random numbers are used in determining component values in only one of the parts, and further wherein for encoding the previously used random numbers the authenticator module (14) and one or more Bloom filter modules (11 12) are configured so that when an upper limit is reached for the one of the parts, another of the parts is reset.